Law Enforcement Directive Implementation Country Report: Germany

Sebastian Golla and Charlotte Korenke

EDRi
European Digital Rights

Law Enforcement Directive Implementation Country Report: in Germany

Sebastian Golla/Charlotte Korenke

TABLE OF CONTENTS

1. Introduction

In Germany, the Data Protection Law Enforcement Directive (EU) 2016/680 (LED) was implemented both at the federal level and the state level in each of the sixteen German *Bundesländer.*[1] While federal law contains regulations on criminal prosecution, state law regulates the powers and tasks of the police and other security authorities in the preventive field. This report focuses on the implementation of the LED for the German police at the state level, which is the most detailed implementation of the directive that took place in Germany. The report primarily looks at the police law of the *Bundesland* Hamburg as an example, but also uses the implementation in other states as a reference in certain areas.

In German police law, there are essentially two approaches to implementing the LED.[2] Firstly, most *Bundesländer* have implemented the requirements of the LED in their existing police laws.[3] These contain sections on police data processing, which, in addition to the corresponding police powers, also contain regulations on data subjects' rights and procedural requirements. Secondly, there are a few *Bundesländer* that have largely implemented the requirements of the LED in specific laws, which only regulate police data processing.[4] Both approaches have in common that the provisions of the police laws or the laws on police data processing can be supplemented by the provisions of the general data protection laws of the *Bundesländer*. These contain general regulations on the implementation of the LED, which must be observed if there are no special regulations for the police sector.

In general, regarding the German implementation of the LED at both state and federal levels, legislators have adopted relatively few new regulations based on the requirements of the directive that go beyond a literal transposition of its provisions.[5]

Hamburg's state law, which is the focus here, has chosen the second method of implementing the LED. However, it should be noted that even before its implementation, Hamburg already had a special law regulating police data processing: the Law on Police Data Processing from 2 May 1991.[6] As part of the LED implementation process, this law was replaced by the Police Data Processing Act from 12 December 2019 (HmbPolDVG).[7]

This report will look at the areas of data subject rights (II.), the processing of sensitive personal data (III.), the alignment of the legal bases for data processing (IV.), and changes in police law concerning new technologies and big data (V.) with regard to the implementation of the LED. It concludes with a brief summary (VI.).

2. Data subject rights

Hamburg's former Law on Police Data Processing from 2 May 1991 already contained some provisions on data subject rights. However, when the LED was implemented in the new HmbPolDVG, the structure of the data subject rights was aligned with the structure of the Directive. Now sections 66-71 HmbPolDVG specify the rights of data subjects and exceptions thereto.

---

[1] The *Bundesländer* (singular *Bundesland*) are the sixteen federated states of Germany.
[2] See, for an overview of the implementation approaches, *Arzt*, Die EU-JI-Richtlinie im deutschen Polizeirecht, Bürgerrechte & Polizei/CILIP 127 (Dezember 2021), 43 (45 f.); for an overview of implementation laws *Müller/Schwabenbauer*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Ed. 2021, G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht Rn. 560 ff.
[3] For example, Berlin, Hesse and North Rhine-Westphalia.
[4] Hamburg, Saarland and Saxony.
[5] Cf. *Arzt*, Bürgerrechte & Polizei/CILIP 127 (Dezember 2021), 43 (45 f.).
[6] Gesetz über die Datenverarbeitung der Polizei from 2 May 1991, HmbGVBl. p. 187.
[7] Gesetz über die Datenverarbeitung der Polizei from 12 December 2019, HmbGVBl. p. 485.

2.1 The right to individual notification

In addition to the general information provided by the data processing authorities, Art. 13(2) LED stipulates that Member States shall provide by law for the controller to individually notify the data subject, in specific cases, and give them further information to enable the exercise of their rights.

Section 68(1) HmbPolDVG contains a general provision for individual notification. This corresponds almost exactly to Art. 13(1,2) LED; in addition to the general information, the data subject is to be provided with the legal basis of the processing, and the storage period applicable to the data or, if this is not possible, the criteria for determining this period. Where applicable, they shall also be provided with information on the categories of recipients of the data. Where necessary and in particular where the personal data is collected without the knowledge of the data subject, they shall be provided with further information.

The specific instances in which data subjects are to be provided with further information according to HmbPolDVG are those in which data is collected in secret. In these cases, data subjects already had to be notified about the data collection prior to the implementation of the LED, but did not have a right to such extensive information.[8] The right to notification is regulated in the respective legal bases for data processing. For example, according to sections 21(5) and 22(7) HmbPolDVG, those affected by data collection through the covert use of technical means, i.e. in particular those affected by surveillance using hidden cameras or microphones, must be notified after the end of the measure. Pursuant to section 26(4) HmbPolDVG, authorities are obliged to notify those affected by telecommunications surveillance measures, source telecommunications surveillance and the processing of traffic and usage data after the end of the measure. Furthermore, according to section 28(2) and 29(4), those affected by data processing through the use of undercover investigators or informants must be notified after the end of the measure; this applies only where it is possible to do so without jeopardising the possibility of further use of the undercover investigator or informer (see below).

Pursuant to section 31(4), persons who have been put under police observation must also be informed of this after the measure has been completed, as well as people whose subscriber data (*Bestandsdaten*)[9] has been processed by the police (section 27(4)). There is, however, no obligation to notify them about further steps in data processing after the collection, even though data subjects usually do not learn about that in any other way.[10]

2.2 Exceptions to data subject rights

The rights of data subjects under the Directive do not apply without restriction; Member States may provide for far-reaching exceptions. Hamburg, like the other German *Bundesländer*, has made use of this. Exceptions to the right to information were previously regulated generally in the Hamburg Data Protection Act, and are now contained specifically in provisions on the individual rights of data subjects in the HmbPolDVG.

A number of restrictions are regulated jointly with regard to the right to notification and the right to access. Both the right to access and the right to notification can be restricted in compliance with Art. 13(3) LED, if providing the information would endanger the purpose of the measure, the existence of the state, or of life, bodily integrity or freedom of a person (sections 68(2) and 69(4) HmbPolDVG).

---

[8] *Müller/Schwabenbauer*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Ed. 2021, G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht Rn. 1066.

[9] Data collected by telecommunications service providers that is necessary for the establishment, content design, amendment or termination of a contract, in particular the name and address of the customer.

[10] *Arzt*, Die EU-JI-Richtlinie im deutschen Polizeirecht, Bürgerrechte & Polizei/CILIP 127 (December 2021), 43 (47 f.).

According to sections 68(2) and 69(4) HmbPolDVG, where the deployment of undercover investigators and police informers (*V-Leute*) is concerned, information shall only be provided when it is possible to do so without jeopardising the possibility of further use of the undercover investigator or informer. If there is a criminal investigation into the same facts, the data subject shall be notified or information shall be provided only in consultation with the prosecutor's office and as soon as the status of the investigation permits (sections 68(2) and 69(4) HmbPolDVG).

Sections 68(4) and 69(5) HmbPolDVG include a general exception for data either originating from the intelligence services or other agencies of the Federal Ministry of Defence, insofar as the security of the federal state (*Sicherheit des Bundes*) is concerned, or the transfer of data to these authorities. Information may only be provided, and data subjects may only be notified if the intelligence services consent. This restriction of data subject rights already existed in a very similar form prior to the implementation of the LED in section 18(5) HmbDSG 1990.[11] In the old version, however, it included other authorities in addition to the intelligence services. The reason given for including this exception in the new law was that the police authority processing the data could not typically know whether that kind of information could endanger the success of measures taken by these authorities.[12] However, this general exception appears to be very broad: in some cases, there may be safety reasons that justify this restriction, but there needs to be a case-by-case assessment.[13]

The right to notification may be restricted in some further instances. According to section 68(1) HmbPolDVG, the notification shall not be made if it conflicts with the overriding legitimate interests of a data subject. Furthermore, a data subject against whom the measure is not directed may not be notified according to section 68(1) HmbPolDVG if they are only insignificantly affected by the measure and it can be assumed that they have no interest in being notified. A data subject may also not be notified according to section 68(1) HmbPolDVG if their identity is unknown and investigations to establish their identity are deemed unnecessary, taking into account the intensity of the interference of the measure against this person, the effort required to establish their identity and the resulting adverse effects on them or other persons.

According to section 68(3) HmbPolDVG, notification can be definitively waived with the approval of a court five years after the end of the measure if the conditions for notification are highly unlikely to occur in the future, the conditions for deletion are met by both the police and the recipients of data transfers, and the data has been deleted.

The HmbPolDVG further contains restrictions on the right of access if providing the information would involve a disproportionate effort. Section 69(2) HmbPolDVG includes an exception from the right to access for personal data that is processed only because it may not be erased due to statutory retention requirements, or that is used exclusively for the purposes of data backup, data protection control or ensuring the proper operation of a data processing system. In these cases, the controller may refrain from providing the information if it would require a disproportionate effort, and processing for other purposes is excluded by appropriate technical and organisational measures. Before the implementation of the LED, section 18(2) HmbDSG 1990 contained almost the same exception, even though the requirement of disproportionate effort was added.

A similar exception is contained in section 69(2) HmbPolDVG: if data cannot be searched automatically and the data subject does not provide any information that would enable the data to be found, then information may not be provided if the effort required to provide it is disproportionate to the data subject's interest. Instead, the data subject may be granted access to the file. A similar regulation existed under the previous legal situation in section 18(3,4) HmbDSG 1990.[14] The right to erasure contains such an exception as well: if data can only be erased with disproportionate effort, its processing can be restricted in accordance with sections 70(2) and 59(4)

[11] Hamburgisches Datenschutzgesetz of 5 July 1990, HmbGVBl. 1990, p. 133.
[12] Bürgerschaft der Freien und Hansestadt Hamburg, Entwurf des Dritten Gesetzes zur Änderung polizeirechtlicher Vorschriften, Bürgerschafts-Drs. 21/17906, p. 78.
[13] *Golla*, Datenschutzrechtliche Schattengewächse in den Ländern, KriPoZ 2019, 238 (241); *Arzt*, Die EU-JI-Richtlinie im deutschen Polizeirecht, Bürgerrechte & Polizei/CILIP 127 (December 2021), 43 (48).
[14] Bürgerschaft der Freien und Hansestadt Hamburg, Entwurf des Dritten Gesetzes zur Änderung polizeirechtlicher Vorschriften, Bürgerschafts-Drs. 21/17906, p. 79.

No. 4 HmbPolDVG. This has no basis in the Directive:[15] according to Art. 16(3) of the LED, the processing of data may only be restricted instead of erased if the accuracy or inaccuracy of the data cannot be established or if the data must be retained for evidentiary purposes.

3. Sensitive personal data and the requirement of strict necessity

Art. 10 LED lays down requirements for the processing of special categories of personal data. Most importantly, the processing of sensitive data shall be allowed where it is authorised by Union or Member State law and where it is strictly necessary and subject to appropriate safeguards for the rights and freedoms of the data subject.

In section 2(21) HmbPolDVG, "special categories of personal data" are defined as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or other criteria set out in Art. 10 of Directive (EU) 2016/680".[16] Unlike in the LED, biometric data is not directly included in the definition, but via reference to Art. 10 LED. The LED's definition of biometric data is adopted almost word for word in section 2(19) HmbPolDVG, which states that biometric data is "personal data relating to the physical, physiological or behavioural characteristics of a natural person, obtained using specific technical procedures, which allow or confirm the unique identification of that natural person, in particular facial images or dactyloscopic data".

3.1 Requirements for processing in section 4 HmbPolDVG

The particular requirements for processing special categories of data according to Art. 10 LED are implemented in section 4 HmbPolDVG.

According to par. 1 of the provision, the processing of sensitive data is permitted if it is strictly necessary in order to fulfil police tasks or for the purposes of self-protection. This wording can also be found in federal law and in various other state laws.[17] The purposes for which sensitive data may be processed are specified in very general terms: the tasks of the police are the prevention of imminent threats to public safety and order and the elimination of disruptions to public safety and order (section 3 Hamburg Law for the Protection of Public Safety and Order). The explanatory memorandum to the law mentions storing information regarding affiliation with dangerous radical or extremist political groups as an example of data processing necessary to fulfil police tasks.[18] Section 4 HmbPolDVG does not explicitly state that sensitive data may also be processed for the purpose of protection of the vital interest of the data subject or of another natural person as mentioned in Art. 10 (b) LED. But according to the explanatory memorandum, the protection of these interests is among the police tasks for which sensitive data may be processed.[19] There is no legal definition of "self-protection",[20] which is also mentioned as a purpose; the explanatory memorandum cites data concerning a serious risk of infection as an example.[21]

Because these objectives are kept quite vague, it is debatable whether section 4(1) HmbPolDVG and the corresponding provisions in other laws are suitable as legal bases for the processing of

[15] *Golla*, Stellungnahme zu dem Entwurf des Dritten Gesetzes zur Änderung polizeirechtlicher Vorschriften, Drucksache 21/17906, p. 10; *Bäcker*, Die Datenschutzrichtlinie für Polizei und Strafjustiz und das deutsche Eingriffsrecht, in: Hill/Kugelmann/Martini, Perspektiven der digitalen Lebenswelt, 2017, p. 63 (82).
[16] All translations of the HmbPolDVG have been made by the authors.
[17] E.g. Section 46 Federal Data Protection Act; section 54(1) sentence 2, section 3 SächsDSUG (Saxony).
[18] Bürgerschaft der Freien und Hansestadt Hamburg, Entwurf des Dritten Gesetzes zur Änderung polizeirechtlicher Vorschriften, Bürgerschafts-Drs. 21/17906, p. 46.
[19] Bürgerschaft der Freien und Hansestadt Hamburg, Entwurf des Dritten Gesetzes zur Änderung polizeirechtlicher Vorschriften, Bürgerschafts-Drs. 21/17906, p. 46.
[20] *Arzt*, Polizeiliche Verarbeitung "besonderer Kategorien personenbezogener Daten" – Zur Umsetzung der Richtlinie (EU) 2016/680 in Deutschland, DÖV 2023, 991 (1001).
[21] Bürgerschaft der Freien und Hansestadt Hamburg, Entwurf des Dritten Gesetzes zur Änderung polizeirechtlicher Vorschriften, Bürgerschafts-Drs. 21/17906, p. 46.

special categories of personal data. According to the explanatory memorandum to the law, section 4 HmbPolDVG is intended to be such a legal basis.[22] On the other hand, it can be argued that intrusive measures, such as the processing of sensitive data, require a legal basis that complies with the constitutional principles of certainty and clarity,[23] and clearly sets out the circumstances under which data may be collected, the purposes for which it may be used, and the rights of the data subjects.[24] If read on its own, it seems questionable whether section 4(1) HmbPolDVG meets these requirements.[25] At least it is widely recognised that particularly intrusive measures with a wide range, such as facial recognition in public spaces, cannot be legitimised by the provision.[26]

The requirement of strict necessity has been taken from the directive in its original wording. German police law previously did not recognise the concept of strict necessity, only that of necessity. According to the explanatory memorandum, strict necessity is to be assumed if no reasonable alternative or compensatory measures are available to achieve a legitimate objective, whereas necessity means that there are no milder means to achieve the objective.[27] However, the explanatory memorandum dates from 2019; in 2023, the CJEU established additional criteria for strict necessity, including the seriousness of the crime and a stricter interpretation of data protection safeguards.[28] These have not yet found their way into the understanding of the Hamburg law.

Section 4(2) HmbPolDVG regulates the appropriate safeguards for the rights and freedoms of data subjects required under Art. 10 LED. It states that where special categories of data are processed, appropriate safeguards for the data subject's rights and freedoms must be provided. Possible safeguards are listed as examples. In line with recital 37 LED, where examples of safeguards include the possibility to adequately secure the data collected and stricter rules on the access of staff from the competent authority, section 4(2) HmbPolDVG mentions "specific requirements for data security or data protection control" and the restriction of staff access to the personal data. Other possible safeguards include: special deadlines within which it must be reviewed whether the data can be deleted (*Aussonderungsprüffristen*); raising awareness among those involved in data processing operations; processing the data separately from other data; pseudonymisation of personal data; the encryption of personal data; and specific procedural rules ensuring the lawfulness of processing when data is transmitted or processed for other purposes. A ban on the transmission of data, as proposed in recital 37 LED, is not mentioned.[29] The same list of possible appropriate safeguards is included in the corresponding provisions of most other states. The listed measures are exemplary and non-binding;[30] the specific design is left to the discretion of the authority processing the data.[31] However, such an internal specification by the authorities is not available to data subjects and therefore contradicts the transparency requirement stipulated by recital 26 LED.[32]

---

[22] Bürgerschaft der Freien und Hansestadt Hamburg, Entwurf des Dritten Gesetzes zur Änderung polizeirechtlicher Vorschriften, Bürgerschafts-Drs. 21/17906, p. 45.
[23] See below, IV. 1.
[24] *Arzt*, Polizeiliche Verarbeitung "besonderer Kategorien personenbezogener Daten" – Zur Umsetzung der Richtlinie (EU) 2016/680 in Deutschland, DÖV 2023, 991 (995).
[25] *Arzt*, Polizeiliche Verarbeitung "besonderer Kategorien personenbezogener Daten" – Zur Umsetzung der Richtlinie (EU) 2016/680 in Deutschland, DÖV 2023, 991 (995).
[26] *Petri*, Biometrie in der polizeilichen Ermittlungsarbeit am Beispiel der automatisierten Gesichtserkennung, GSZ 2018, 144 (146); *Mysegades*, Keine staatliche Gesichtserkennung ohne Spezial-Rechtsgrundlage, NVwZ 2020, 852 (854).
[27] Bürgerschaft der Freien und Hansestadt Hamburg, Entwurf des Dritten Gesetzes zur Änderung polizeirechtlicher Vorschriften, Bürgerschafts-Drs. 21/17906, p. 45.
[28] CJEU, Judgment of 26 January 2023, C-205/21 par. 126
[29] *Arzt*, Polizeiliche Verarbeitung "besonderer Kategorien personenbezogener Daten" – Zur Umsetzung der Richtlinie (EU) 2016/680 in Deutschland, DÖV 2023, 991 (997).
[30] Bürgerschaft der Freien und Hansestadt Hamburg, Entwurf des Dritten Gesetzes zur Änderung polizeirechtlicher Vorschriften, Bürgerschafts-Drs. 21/17906, p. 46.
[31] *Arzt*, Polizeiliche Verarbeitung "besonderer Kategorien personenbezogener Daten" – Zur Umsetzung der Richtlinie (EU) 2016/680 in Deutschland, DÖV 2023, 991 (996); *Aden*, Besserer Datenschutz auch für Polizei und Strafjustiz?, vorgänge 2018, 93 (99).

3.2 Specific legal bases for the processing of special categories of data

In addition to the comprehensive clause in section 4, the HmbPolDVG only contains one provision regulating two specific ways of processing sensitive data. Section 16 HmbPolDVG regulates measures for the purpose of identification (*erkennungsdienstliche Maßnahmen*) and the identification of unknown dead bodies through the analysis of DNA samples. This regulation already existed prior to the implementation of the LED and has only been slightly changed to adapt to the new terminology of data protection law. Identification measures as defined in section 16(3) HmbPolDVG include the collection of fingerprints and palm prints, the taking of photographs, the determination of externally perceptible features and the taking of measurements, i.e. various forms of processing biometric data. Such measures may be carried out either for the purpose of establishing identity in specific cases: first, if this is not possible by other means or only with considerable difficulty; second, for the preventive combating of criminal offenses if the person in question is suspected of having committed a punishable offense and there is a risk of further criminal offenses being committed due to the nature or execution of the offense and the personality of the person concerned. The criterion of personality does not appear in the regulations of most other federal states and has not been defined more precisely by case law. In this context, courts take into account, for example, previous convictions, behaviour after committing the offence, and mental disorders.[33]

As a safeguard, these measures may only be ordered by "specially authorised officers". DNA samples may be collected and analysed according to section 16(4) HmbPolDVG if it is not possible to otherwise identify a dead body. For that purpose, the DNA identification pattern may be processed in a filing system but cannot be used for any other purposes and has to be deleted after the measure has been completed. Various other state laws also permit the collection and analysis of DNA samples to identify persons in a state of helplessness[34] or to prevent criminal offences.[35] To protect the rights of the person affected, the molecular genetic analysis has to be ordered by a judge and is to be carried out by court-appointed experts not affiliated with the authority that commissioned the analysis. They must take technical and organisational measures to ensure that further molecular genetic examinations and unauthorised access by third parties cannot take place, and the expert is not to be provided with identifying information on the person concerned, such as name, address, or date of birth.

Section 34(6) HmbPolDVG contains a legal basis for the storage of additional personal information on persons on whom a data record has already been created if it is necessary for the protection of this person or for the protection of police officers, or if the information is suitable for the protection of third parties or for obtaining investigative leads. Sentence 2 of the provision states that the requirements of Section 4 HmbPolDVG must be abided by if the data stored in this context cover special categories of personal data. However, it does not mention specific safeguards for the rights and freedoms of the person concerned in these cases.

---

[32] *Arzt*, Polizeiliche Verarbeitung "besonderer Kategorien personenbezogener Daten" – Zur Umsetzung der Richtlinie (EU) 2016/680 in Deutschland, DÖV 2023, 991 (996 f.)

[33] Cf. on the previous section 7 HmbPolDVG: Hamburgisches Oberverwaltungsgericht, Judgment of 11 April 2013 – 4 Bf 141/11, section 86.

[34] Cf. section 183a par. 2, 3 SchlHLVwG (Schleswig-Holstein), section 15a NPOG (Lower Saxony), section 11a RhPfPOG (Rhineland-Palatinate), section 21a ASOG (Berlin).

[35] Cf. section 19 HSOG (Hesse), section 32a BayPAG (Bavaria).

3.4 Other provisions concerning special categories of data

Section 9(2,3) HmbPolDVG implements the ban on making automated individual decisions based on special categories of data unless appropriate measures are taken to protect the data subject's legal and legitimate interests, and the ban on discriminatory profiling laid down in Art. 11 LED. The wording of Art. 11(2,3) of the Directive is adopted almost in full. However, the term "rights and freedoms" has been replaced by "legal interests", and the text has thus been adapted to German legal terminology.

The provision in Art. 29 LED regarding the security of data processing, according to which a level of security appropriate to the risk must be ensured, in particular with regard to the processing of sensitive data, has been implemented in section 54 HmbPolDVG.

4. Alignment of the legal bases for data processing

4.1 Adaptation of the legal bases for data processing

Overall, the implementation of the LED had little influence on the legal bases for police data processing in German law. This is largely because a differentiated discourse on the limits of police powers of intervention had already taken place in Germany before the LED was implemented, and the competences in the area of data processing were also repeatedly reviewed under constitutional law.

The main requirements for national regulations on police competences for data processing are set out in Art. 8 and Art. 10 LED. Art. 8(1) states that "Member States shall provide for processing to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Art. 1 (1) and that it is based on Union or Member State law". In the implementation process, it was widely considered that the requirements of Art. 8(1) LED were already met in German police law before the LED came into effect.[36] Accordingly, the requirements of the LED for legal bases for police data processing were not considered as very strict in the national debate.[37]

The German Federal Constitutional Court recognised the right to informational self-determination under Art. 2(1) in conjunction with Art. 1(1) of the Basic Law in its 1983 census ruling.[38] Since then, in Germany, it has been recognised that a legal basis is required for any processing of personal data by a state authority following the general principle of statutory reservation (*Vorbehalt des Gesetzes*). In the case of public bodies like the police, such a legal basis must – in accordance with the principle of proportionality – at least presuppose that the data processing is necessary for the performance of their tasks.

This understanding is also reflected in section 11 HmbPolDVG and its predecessor provisions in the Hamburg Law on Police Data Processing, which require that the respective data processing is necessary for the fulfilment of police tasks. Comprehensive clauses such as section 11 HmbPolDVG exist in the police laws of all federal states. They form the legal bases for data processing that is only slightly intrusive, i.e. does not significantly affect the rights of the data subjects. Everyday processing operations, such as the storage of data in police databases or their retrieval, can be based on them.

---

[36] Cf. *Bäcker*, Die Datenschutzrichtlinie für Polizei und Strafjustiz und das deutsche Eingriffsrecht, in: Hill/Kugelmann/Martini, Perspektiven der digitalen Lebenswelt, 2017, p. 63 (69 f.); *Müller/Schwabenbauer*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Ed. 2021, G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, par. 463.

[37] *Bäcker/Hornung*, EU-Richtlinie für die Datenverarbeitung bei Polizei und Justiz in Europa - Einfluss des Kommissionsentwurfs auf das nationale Strafprozess- und Polizeirecht, ZD 2012, 147 (150).

[38] Federal Constitutional Court, Judgment of the First Senate from December 15, 1983 – 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83.

Art. 8(2) LED additionally requires that "Member State law regulating processing within the scope of this Directive shall specify at least the objectives of processing, the personal data to be processed and the purposes of the processing". This provision can be interpreted as a requirement of certainty for the legal basis of police data processing. It requires legislators to pay particular attention to the purpose and objectives of data processing. LED recital 33 more specifically states that a "legal basis or legislative measure should be clear and precise and its application foreseeable for those subject to it, as required by the case-law of the Court of Justice and the European Court of Human Rights".

In the German implementation of the LED and the accompanying discussion, Art. 8(2) LED was not interpreted in such a way that stricter requirements for the specificity of legal bases for data protection were derived from the provision than under the previously established requirements of German constitutional law.[39]

German constitutional law has already imposed comparatively strict requirements on the specificity of the police's data processing powers since the 1983 census ruling. Since then, the requirements of fundamental rights protection, which are primarily based on the principles of proportionality and certainty, have been repeatedly discussed based on specific constellations of police data processing. In several cases, this has led to special data processing powers being introduced in police laws or adapted in accordance with constitutional requirements. Corresponding discussions concerned, for example, data comparison in the form of dragnet searches,[40] police license plate recognition[41] and, most recently, the use of AI in police data mining.[42]

How specific the requirements for police data processing should be and how high the thresholds for this must be essentially depends on how intensively processing interferes with the rights of the data subject. The German Federal Constitutional Court has developed detailed criteria for determining the intensity of interference with specific measures. These include the scope of a measure, the existence of data with particular personal relevance (which may be the case with special personal data within the meaning of Art. 10 LED), the probability of follow-up measures and the hidden nature of the interference.[43]

4.2 The problem of consent

A particular problem arose in the implementation of the LED and the revision of the legal bases for police data processing with the question of whether consent can be considered as a suitable legal basis in the relationship between the police and citizens. Section 5 HmbPolDVG provides for the possibility of consent as a suitable legal basis, as do other police laws.

In principle, consent as a legal basis in the area of police activity is problematic because it must be given voluntarily. If someone is confronted with police measures, they regularly find themselves under pressure. They will expect that if they do not consent to data processing, they will be obliged to tolerate or actively participate in it, and that they will be at a disadvantage if they refuse.[44]

In its articles, the LED does not mention consent as a possible basis for data processing. However, recitals 35 and 37 LED suggest that consent is not completely excluded as a basis for processing. Recital 35 focuses on the situations in which consent cannot be given and gives the impression that consent is excluded as a basis for processing in many areas.[45] However, according to recital 35 LED, Member States should not be precluded "from providing, by law, that the data subject may

[39] *Bäcker*, Die Datenschutzrichtlinie für Polizei und Strafjustiz und das deutsche Eingriffsrecht, in: Hill/Kugelmann/Martini, Perspektiven der digitalen Lebenswelt, 2017, p. 63 (69 f.).
[40] Federal Constitutional Court, Decision of the First Senate from 4 April 2006 – 1 BvR 518/02.
[41] Federal Constitutional Court, Decision of the First Senate from 18 December 2018 – 1 BvR 142/15.
[42] Federal Constitutional Court, Judgment of the First Senate from 16 February 2023 – 1 BvR 1547/19, 1 BvR 2634/20; see in more detail under V.
[43] See for a current summary *Kugelmann/Buchmann*, Der Algorithmus und die Künstliche Intelligenz als Ermittler, GSZ 2024, 1 (5 ff.).
[44] For further details see *Golla/Skobel*, „Sie haben doch nichts zu verbergen?" – Zur Möglichkeit einer Einwilligung in die Datenverarbeitung im Geltungsbereich der Richtlinie (EU) 2016/680. GSZ 2019, 140 ff.

agree to the processing of his or her personal data for the purposes of this Directive, such as DNA tests in criminal investigations or the monitoring of his or her location with electronic tags for the execution of criminal penalties". According to recital 37 LED, a legal provision may permit the processing of special categories of personal data if the data subject has expressly "agreed".

One possible conclusion from this is that consent can only be the legal basis for data processing within the scope of the LED if it is expressly regulated. The question is whether consent can only be regulated as a legal basis for data processing in the scope of the application of the LED with regard to specific cases and measures, or also as a general clause for all cases of data processing.[46]

The regulations on consent in the current police laws – such as Section 5 HmbPolDVG – predominantly provide for comprehensive clauses, according to which the processing of personal data by the police should normally be possible based on consent. Those comprehensive clauses do not refer to specific cases or types of data that can be covered by consent. It is questionable whether this regulation method is sufficient to meet the requirements of the LED.

Section 5(1) HmbPolDVG requires that consent must have been given voluntarily. According to this section of the provision, "when assessing whether consent was given voluntarily, [...] the circumstances under which it was given must be taken into account". Information about the consequences of refusing consent is also to be provided in individual cases. The request for consent, if made in writing, must be made in an understandable and easily accessible form in clear and simple language (par. 3). Finally, the data subject expressly has the right to withdraw their consent at any time (par. 4).

5. New technologies and big data

In Germany, so far, only a small number of police authorities use methods of artificial intelligence or similar tools for the mass analysis of available data. Specific applications have been tested and implemented at federal and state levels.[47] In addition to these, efforts are being made to use artificial intelligence on a broader scale. Such efforts can be observed in North Rhine-Westphalia, Bavaria and Hesse. All three *Bundesländer* have amended their police laws and use new research and analysis platforms based on Palantir Gotham.[48] Among them, Hesse is the most advanced in terms of both creating the legal basis and technical implementation. The police in Hesse use a platform called HessenDATA to combat crime.[49] It can combine information from different databases in a complex way. However, there is little publicly available information about the exact technical functioning of this platform.

The Hessian legislator has created a legal basis for the automated analysis of data within the framework of this platform in section 25a of the Hessian Law on Public Safety and Order (Hessisches Gesetz über die öffentliche Sicherheit und Ordnung, HSOG). A provision almost identical in wording to section 25a HSOG can be found in section 49 HmbPolDVG, although the police in Hamburg do not currently use a platform for automated data analysis. As summarised by the German Constitutional court, both provisions "provide a specific statutory basis for linking previously unconnected automated databases and data sources in analysis platforms and permitting systematic access of data across sources through searches. The provisions authorise

[45] *Johannes/Weinhold*, Das neue Datenschutzrecht bei Polizei und Justiz, 2018, section 1 par. 154.
[46] For the need for a specific regulation for certain measures see *Bäcker*, Die Datenschutzrichtlinie für Polizei und Strafjustiz und das deutsche Eingriffsrecht, in: Hill/Kugelmann/Martini, Perspektiven der digitalen Lebenswelt, 2017, p. 63 (71); *Golla*, Datenschutzrechtliche Schattengewächse in den Ländern, KriPoZ 2019, 238 (240); *Johannes/Weinhold*, Das neue Datenschutzrecht bei Polizei und Justiz, 2018, section 1 par. 157.
[47] See for examples *Kugelmann/Buchmann*, Der Algorithmus und die Künstliche Intelligenz als Ermittler, GSZ 2024, 1 (2).
[48] The Bavarian platform is named VeRA (*Verfahrensübergreifenden Recherche- und Analyseplattform*); see for more information: https://www.polizeiaufgabengesetz.bayern.de/faq/index.php. The platform used by the police in North Rhine-Westphalia is called DAR (*Datenbankübergreifende Recherche und Analyse*); see for more information: https://www1.wdr.de/nachrichten/landespolitik/palantir-fahndungserfolge-100.html.
[49] See for an introduction: https://police-it.net/hessendata-and-its-impact-on-personal-data-protection-and-privacy.

the police to process stored personal data through automated data analysis (Hesse) or automated data interpretation (Hamburg), subject to a case-by-case assessment, in order to prevent serious criminal acts [...] or to avert dangers to certain legal interests (second alternative). Section 2 of both provisions provides that relationships or connections between persons, groups of persons, institutions, organisations, objects or matters can thereby be established, insignificant information and intelligence can be filtered out, insights generated can be matched to known facts and stored data can be analysed."[50]

In addition to section 25a HSOG and section 49 HmbPolDVG, there are only individual provisions aimed at the use of AI and big data analysis in the federal Antiterrorism Data Act,[51] the Police Act of North Rhine-Westphalia,[52] and the Bavarian Law on Police Tasks.[53] Section 25a HSOG and section 49 HmbPolDVG were the subject of two constitutional complaints that were heard jointly by the Federal Constitutional Court in December 2022.

In its ruling of 16 February 2023 (case number 1 BvR 1547/19, 1 BvR 2634/20), the court declared the respective provisions unconstitutional insofar as they related to the prevention of criminal acts.[54] The court ruled that the provisions did not provide for a sufficiently high threshold, considering the far-reaching possibilities of automated data processing that they would open up. Therefore, the provisions did not constitute a suitable justification for the possible interference with the constitutionally protected right to informational self-determination.[55]

Although Section 49 HmbPolDVG was introduced into Hamburg's police law together with the implementation of the LED, the provision is not closely interlinked with the requirements of the LED. The requirements that the LED places on data protection impact assessments, purpose limitation, differentiation between different categories of data and human involvement in decisions are essentially implemented in laws[56] that stand alongside the data processing powers of the police.

This also applies to Section 49 HmbPolDVG. For example, the regulation does not explicitly require a data protection impact assessment for the establishment of an AI-supported platform for automated data analysis. However, this requirement can be derived from the general provision of section 57 HmbPolDVG, which requires an impact assessment to be carried out for particularly risky processing operations, especially when using new technologies.

Section 49 HmbPolDVG was criticised for the lack of safeguards relating to the use of AI tools or other powerful tools for data analysis, as highlighted in the constitutional complaint against the provision.[57] However, the Federal Constitutional Court did not rule on the procedural safeguards, since in the court's view the complainants had not asserted their right to complain clearly enough in this respect. It should be noted that the lack of safeguards is not exclusively a problem of national (constitutional) law. Art. 10 (regarding the processing of special categories of personal data) and Art. 11(1) LED (regarding automated individual decision-making) also demand appropriate safeguards for the rights and freedoms of the data subject. Insofar as these regulations are applicable, the shortcomings in establishing specific safeguards for AI use could therefore also violate European Union law.

---

[50] Federal Constitutional Court, Press Release No. 18/2023 of 16 February 2023 (English), available at: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2023/bvg23-018.html.
[51] Section 6a.
[52] Section 23 par. 6.
[53] Section 61a.
[54] The provisions also contain a second alternative relating to the aversion of dangers to certain legal interests, which was not declared unconstitutional.
[55] For a summary in English see Federal Constitutional Court, Press Release No. 18/2023 of 16 February 2023, available at: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2023/bvg23-018.html; see for a critical assessment *Vasel*, Verfassungsgerichtliche Fesseln? – Das Karlsruher Urteil zur automatisierten Datenanalyse, NJW 2023, 1174 ff.
[56] The LED was mainly implemented in legislative acts adopted by parliaments.
[57] See for the full text (in German): https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/Trojaner-fuer-den-Verfassungsschutz/Beschwerdeschrift-Gesellschaft_fuer_Freiheitsrechte-2020-Trojaner_fuer_Verfassungsschutz-Freiheit_im_digitalen_Zeitalter.pdf.

Firstly, it should be noted that there are no provisions in German law that clearly define the necessary quality of data for automated analysis. The general provisions on data quality essentially reflect the wording of the Directive, but do not appear to be suitable for deriving specific requirements for action. A review of data quality, particularly before complex analysis, would not only be necessary for the protection of the data subjects, but would also be in the interests of the authorities, as no meaningful results can be expected on the basis of a low-quality database ("trash in – trash out").

Secondly, German law does not contain any regulations that deal with the possible discriminatory effects of automated data analyses or the training of the systems in advance. There are legitimate doubts as to whether data protection law would be the right context for such a regulation. Discrimination against individuals through state measures is not directly covered by data protection law, which tends to apply in the preliminary stages of noticeable harm. Structural discrimination effects are difficult to address through current data protection laws. In any case, however, the risks of discrimination associated with these processes are widely recognised and give reason to address these problems from a legal perspective.

Thirdly, the transparency-creating regulations in connection with powers such as section 49 HmbPolDVG have room for improvement. In principle, data subjects can use requests for information to find out whether data about them has been included in relevant proceedings, unless the police argue that there is a reason for exclusion. However, a proactive notification obligation could also be useful in such cases.

Finally, it should be noted that the restrictions on the permissibility of automated individual decisions under Art. 11 LED have not had a noticeable impact on the legal bases and practices for AI-supported data processing in the German police forces. The requirement of the LED was inserted in the laws implementing the Directive almost word for word, for example in section 9 HmbPolDVG. However, the police forces take the position that the systems currently used and planned only serve to support and prepare human decisions, which is why there would be no decision based solely on automated processing. It is possible to take a critical look at this assumption if the results of AI data evaluations strongly influence subsequent human decisions. In this context, the SCHUFA decision of the CJEU of 7 December 2023 is particularly interesting. This decision concerned Art. 22(1) GDPR, which has very similar content to the laws implementing Art. 11(1) LED (here: section 9 HmbPolDVG). Both provide that the data subject is to have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

The CJEU ruled that section 22(1) GDPR "must be interpreted as meaning that the automated establishment, by a credit information agency, of a probability value based on personal data relating to a person and concerning his or her ability to meet payment commitments in the future constitutes 'automated individual decision-making' within the meaning of that provision, where a third party, to which that probability value is transmitted, draws strongly on that probability value to establish, implement or terminate a contractual relationship with that person."[58]

The assumption that a probability calculation can be a decision in the sense of Art. 22(1) GDPR if it determines people's behaviour (e.g. the approval of a loan) can be transferred to the police sector and Art. 11(1) LED. However, the police essentially control their means of decision support themselves, meaning that they have more opportunities to scrutinise probability calculations than companies who retrieve credit scores from the SCHUFA agency.

In case of measures taken by the police, it would require access to the results of decision-supporting data analysis in their specific form in order to assess if they constitute decisions that are made automatically within the meaning of Art. 11(1) LED. In principle, this access is possible via the rights to information under data protection law, although it is to be expected that the responsible police authorities will invoke exceptions to the obligation to provide information in order to prevent this.

[58] Judgment of the Court (First Chamber) of 7 December 2023 – OQ v Land Hessen, Case C-634/21.

6. Conclusion and Recommendations

6.1 Conclusion

The adjustments to Hamburg's police law examined here can largely be seen as exemplifying those made in various other German states and at federal level as a result of the implementation of the LED.

In their basic outline, the adaptations are characterised by a rather minimally invasive approach. The legal basis for data processing has hardly changed. Adjustments have been made to the principles for the processing of particularly sensitive personal data, whereby only individual terms have been changed. The introduction of new legal bases for complex data analysis was made independently of specific LED requirements. However, a lively debate is underway in the area of AI use by the police in Germany, which was most recently fuelled by the ruling of the Federal Constitutional Court on Section 49 HmbPolDVG in February 2023.

The police laws of Hamburg and other federal states have undergone more detailed amendments with regard to the regulation of data subjects' rights. These were regulated in more detail as a result of the LED. However, the laws provide for various exceptions to the rights to notification, information and erasure, and their compatibility with the LED is thus questionable in some cases.

6.2 Recommendations

The exemptions from the data subject rights should be reduced. In particular, data subjects' rights should not be restricted due to excessive administrative burdens. In addition, the very broad exception for the involvement of intelligence services should be limited to cases where there are security risks.

The legal bases for police data processing could be improved through more specific regulations. It is doubtful whether the broad possibilities of data processing on the basis of consent meet the requirements of the LED. AI-supported data analysis already requires more precise regulations in accordance with the requirements of national law (regarding certainty and proportionality). These should be supplemented by safeguards for the rights and freedoms of the data subject. Finally, it would be advisable to create more specific legal bases for the processing of sensitive data, in which safeguards for the rights of data subjects, in particular, are more clearly defined. In comparison with other Member States, the implementation of the LED in Germany is of average quality, based on the assessment of the EU in its report on the transposition of the LED from November 2020.

7. Sources

Aden, Hartmut: Besserer Datenschutz – auch für Polizei und Strafjustiz?, vorgänge 2018, p. 93 ff.

Arzt, Clemens: Die EU-JI-Richtlinie im deutschen Polizeirecht, Bürgerrechte & Polizei/CILIP 127 (December 2021), p. 43 ff.

Arzt, Clemens: Polizeiliche Verarbeitung „besonderer Kategorien personenbezogener Daten" – Zur Umsetzung der Richtlinie (EU) 2016/680 in Deutschland, DÖV 2023, p. 991 ff.

Bäcker, Matthias; *Hornung*, Gerrit: EU-Richtlinie für die Datenverarbeitung bei Polizei und Justiz in Europa – Einfluss des Kommissionsentwurfs auf das nationale Strafprozess- und Polizeirecht, ZD 2012, p. 147 ff.

Bäcker, Matthias: Die Datenschutzrichtlinie für Polizei und Strafjustiz und das deutsche Eingriffsrecht, in: Hill/Kugelmann/Martini, Perspektiven der digitalen Lebenswelt, Baden-Baden 2017, p. 63 ff.

Golla, Sebastian: Stellungnahme zu dem Entwurf des Dritten Gesetzes zur Änderung polizeirechtlicher Vorschriften, Drucksache 21/17906, 13 September 2019.

Golla, Sebastian: Datenschutzrechtliche Schattengewächse in den Ländern – Herausforderungen bei der Umsetzung der JI-Richtlinie für die Polizei, KriPoZ, 2019, p. 241 ff.

Golla, Sebastian/*Skobel*, Eva: „Sie haben doch nichts zu verbergen?" – Zur Möglichkeit einer Einwilligung in die Datenverarbeitung im Geltungsbereich der Richtlinie (EU) 2016/680, GSZ 2019, p. 140 ff.

Johannes, Paul/*Weinhold*, Robert: Das neue Datenschutzrecht bei Polizei und Justiz, Baden-Baden 2018.

Kugelmann, Dieter/*Buchmann*, Antonia: Der Algorithmus und die Künstliche Intelligenz als Ermittler, GSZ 2024, p. 1 ff.

Lisken/Denninger, Handbuch des Polizeirechts, 7. Ed. Munich 2021.

Mysegades, Jan: Keine staatliche Gesichtserkennung ohne Spezial-Rechtsgrundlage, NVwZ 2020, 852 ff.

Petri, Thomas: Biometrie in der polizeilichen Ermittlungsarbeit am Beispiel der automatisierten Gesichtserkennung, GSZ 2018, 144 ff.

Vasel, Justus: Verfassungsgerichtliche Fesseln? – Das Karlsruher Urteil zur automatisierten Datenanalyse, NJW 2023, 1174 ff.

8. Glossary

8.1 Cited Laws

Bavarian Law on Police Tasks of 14 September 1990 (Gesetz über die Aufgaben und Befugnisse der Bayerischen Polizei – BayPAG)

Federal Antiterrorism Data Act of 22 December 2006 (Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern – ATDG)

Federal Data Protection Act of 30 June 2017 (Bundesdatenschutzgesetz – BDSG)

General Administrative Law for the State of Schleswig-Holstein of 2 June 1992 (Allgemeines Verwaltungsgesetz für das Land Schleswig-Holstein – SchlHLVwG)

General Safety and Order Act Berlin of 3 January 2023 (Allgemeines Sicherheits- und Ordnungsgesetz Berlin – ASOG)

Federal Antiterrorism Data Act of 22 December 2006 (Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern– ATDG)

Federal Data Protection Act of 30 June 2017 (Bundesdatenschutzgesetz – BDSG)

Hamburg Data Protection Act of 18 May 2018 (Hamburgisches Datenschutzgesetz – HmbDSG)

Hamburg Law on Police Data Processing of 2 May 1991 (Gesetz über die Datenverarbeitung der Polizei from 2 May 1991)[59]

Hamburg Police Data Processing Act of 12 December 2019 (Gesetz über die Datenverarbeitung der Polizei from 12 December 2019 – HmbPolDVG)[60]

Hessian Law on Public Safety and Order of 14 January 2005 (Hessisches Gesetz über die öffentliche Sicherheit und Ordnung – HSOG)

Lower Saxony Police and Public Order Act Act of 19 January 2005 (Niedersächsisches Polizei- und Ordnungsbehördengesetz – NPOG)

North Rhine-Westphalia Police Act of 25 July 2003 (Polizeigesetz des Landes Nordrhein-Westfalen – PolG NRW)

Police and Public Order Act Rhineland-Palatinate of 10 November 1993 (Polizei- und Ordnungsbehördengesetz Rheinland-Pfalz – RHPfPOG)

Saxon Data Protection Implementation Act of 11 May 2019 (Sächsisches Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 – SächsDSUG)

8.2 Court Cases

Federal Constitutional Court, Judgment of the First Senate of 15 December 1983 – 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83

Federal Constitutional Court, Decision of the First Senate of 4 April 2006 – 1 BvR 518/02

Federal Constitutional Court, Decision of the First Senate of 18 December 2018 – 1 BvR 142/15

Federal Constitutional Court, Judgment of the First Senate of 16 February 2023 – 1 BvR 1547/19, 1 BvR 2634/20

[59] The law on police data processing in Hamburg, which has since expired and was relevant before the LED came into force.
[60] The current law on police data processing in Hamburg, which implements the LED.

Court of Justice of the European Union of 7 December 2023 – OQ v Land Hessen, Case C-634/21 (SCHUFA)

Court of Justice of the European Union, Judgment of 26 January 2023, C-205/21 (Recording of biometric and genetic data by the police)

Press enquiries
press@edri.org

Brussels office
brussels@edri.org

Phone number
+32 2 274 25 70

Visit us

Rue Belliard 12
1040 Brussels
Belgium

Follow us

Mastodon
Facebook
LinkedIn
Youtube
Instagram

EDRi
European Digital Rights