

LANDTAG  
NORDRHEIN-WESTFALEN  
18 WAHLPERIODE

**STELLUNGNAHME  
18/1344**

A14, A09

An den  
Rechtsausschuss  
des Landtags Nordrhein-Westfalen



Dr. iur. Rainer Frank  
Rechtsanwalt · Fachanwalt für Strafrecht  
Compliance Officer (Steinbeis)  
Compliance Auditor (TÜV)

Dr. iur. Niklas Aufermann  
Rechtsanwalt · Fachanwalt für Strafrecht  
Mediator

Dr. iur. Sebastian T. Vogel  
Rechtsanwalt · Fachanwalt für Strafrecht  
Healthcare Compliance Officer (HCO)

Dr. iur. David Albrecht  
Rechtsanwalt · Fachanwalt für Strafrecht

Dr. iur. Leonie Lo Re  
Rechtsanwältin · Fachanwältin für Strafrecht  
Compliance Officer (Steinbeis)  
Compliance Auditor (TÜV)

Dr. iur. Michael Liedke  
Rechtsanwalt

Fabian Breuer  
Rechtsanwalt  
Compliance Officer (Steinbeis)

Dr. iur. Viktor Volkmann, LL.M. (TCD)  
Rechtsanwalt  
Compliance Officer (Steinbeis)  
Zert. Berater Steuerstrafrecht (FeUW)

Dr. iur. Laura Seifert  
Rechtsanwältin

Sophia Hoffmeister  
Rechtsanwältin

Lisa Engelbrecht  
Rechtsanwältin

Potsdamer Platz 8 · 10117 Berlin

Telefon 030/31 86 85-3  
Telefax 030/31 86 85-55  
E-Mail mail@fs-pp.de

www.fs-pp.de

AG ChlbG. – PR 994 B

**07.03.2024**  
63.23

**Antrag der Fraktion der FDP „Persönliche Daten von  
unschuldig Verfolgten müssen sicher und für die Be-  
troffenen nachprüfbar gelöscht werden“ (Drs. 18/5841)  
Anhörung am 13. März 2024**

Sehr geehrte Damen und Herren,

zur Vorbereitung der bezeichneten Anhörung übersende  
ich Ihnen nachfolgend meine schriftliche Stellungnahme.

**I. Zur Löschpflicht**

Das Recht auf informationelle Selbstbestimmung genießt  
Verfassungsrang. Sein wesentlicher Inhalt liegt darin, dass  
sein Inhaber frei über Erhebung, Speicherung, Verwendung  
und Weitergabe der eigenen Daten zu entscheiden. Ein-  
griffe in die informationelle Selbstbestimmung dürfen nicht  
leichtfertig erfolgen, sondern müssen sich stets am Grund-  
satz der Verhältnismäßigkeit messen lassen.<sup>1</sup> Es ist öffent-  
lichen Stellen demnach von Verfassungs wegen grundsätz-  
lich untersagt, personenbezogene Daten über die Grenze  
des Erforderlichen hinaus zu speichern oder auf andere

<sup>1</sup> BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83.

Weise zu verarbeiten. Alleine die theoretische Möglichkeit, die Daten in Zukunft nutzen zu können, rechtfertigt eine weitere Speicherung nicht.

Für die Datenverarbeitung in polizeilichen Systemen finden diese Grundsätze ihre einfachgesetzliche Ausprägung, sofern es den Bereich der Strafverfolgung betrifft, in den §§ 483 ff. StPO und, soweit es die Gefahrenabwehr angeht, in den §§ 22 PolG NRW. Welches Regelungsregime – StPO oder PolG – zur Anwendung kommt, richtet sich nach dem Zweck der (weiteren) Datenverarbeitung: Die Verarbeitung für Zwecke eines bereits anhängigen Strafverfahrens richtet sich nach der StPO. Die Verarbeitung zum Zwecke der Gefahrenabwehr und/ oder für Zwecke künftiger Strafverfahren richtet sich nach den Polizeigesetzen (letzteres über die Verweisung in § 484 Abs. 4 StPO). Die vorliegend zu behandelnde Frage der ordnungsgemäßen Datenlöschung nach Abschluss von Strafverfahren ist somit auf Grundlage des PolG NRW zu beantworten.

§ 32 Abs. 1 PolG NRW bestimmt, dass gespeicherte personenbezogene Daten grundsätzlich zu löschen sind, soweit sie für die Erfüllung der Aufgaben der speichernden Stelle nicht mehr erforderlich sind. Zu diesem Zweck haben die verantwortlichen Stellen Termine festzulegen, zu denen *spätestens* überprüft werden muss, ob eine weitere Datenspeicherung erforderlich ist (§ 22 Abs. 2 S. 5, Abs. 4 S. 1 PolG NRW). Diese Höchstfristen entbinden die verantwortliche Stelle indes nicht von einer einzelfallbezogenen Prüfung der Rechtmäßigkeit der weiteren Datenspeicherung. Aus den vorgenannten verfassungsrechtlichen Vorgaben folgt vielmehr die Verpflichtung der verantwortlichen Stellen, durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass Datensätze mit Personenbezug *unverzüglich* gelöscht werden, sobald diese nicht mehr für die polizeiliche Aufgabenerfüllung benötigt werden.<sup>2</sup> Eine entsprechende Pflicht folgt auch aus Art. 16 Abs. 2 der Richtlinie (EU) 2016/680 (sog. JI-Richtlinie).

Diese Grundsätze hat auch der Europäische Gerichtshof (EuGH) in einem kürzlich ergangenen Urteil aufgegriffen und darauf hingewiesen, dass die JI-Richtlinie gewährleisten soll, dass

*„personenbezogene Daten gemäß den Anforderungen von Art. 4 Abs. 1 Buchst. e dieser Richtlinie nicht länger als erforderlich gespeichert werden.*

---

<sup>2</sup> Müller/Schwabenbauer in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Kap. G Rn. 856.

*Zwar überlässt es die Richtlinie den Mitgliedstaaten, angemessene Fristen für die Dauer der Speicherung festzulegen und zu entscheiden, ob diese Fristen die Löschung dieser Daten oder die regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung betreffen, vorausgesetzt, die Einhaltung dieser Fristen wird durch angemessene Verfahrensvorkehrungen sichergestellt. Für die „Angemessenheit“ dieser Fristen ist jedoch jedenfalls erforderlich, dass sie gemäß Art. 4 Abs. 1 Buchst. c und e der Richtlinie im Licht von Art. 52 Abs. 1 der Charta gegebenenfalls die Löschung der betreffenden Daten ermöglichen, wenn ihre Speicherung im Hinblick auf die Zwecke, die die Verarbeitung gerechtfertigt haben, nicht mehr erforderlich ist.“ (EuGH, Urt. v. 30.1.2024 - C-118/22, Rn. 45).*

Erforderlich ist eine fortdauernde Speicherung nach der Rechtsprechung des EuGH dabei nur, sofern ein „*notwendiger Zusammenhang*“ zwischen den gespeicherten Daten und dem mit der Fortspeicherung verfolgten Ziel (EuGH, Urt. v. 30.1.2024 - C-118/22, Rn. 60).

Allein die *Möglichkeit*, dass die in Polizeidatenbanken gespeicherten Daten einer ehemals beschuldigten Person später noch einmal in anderen Zusammenhängen benötigt werden, rechtfertigt eine weitere Speicherung daher nicht.

Wird ein Ermittlungsverfahren nach § 170 Abs. 2 StPO eingestellt, hat sich die ursprünglich angenommene Verdachtshypothese also im Laufe der Ermittlungen nicht hinreichend verfestigt, ist eine weitere Speicherung der personenbezogenen Daten des ehemals Beschuldigten in der Regel nicht erforderlich im vorgenannten Sinne.

Haben die Ermittlungsbehörden, wozu sie gesetzlich verpflichtet sind, den Sachverhalt „*ausermittelt*“ (§ 160 Abs. 1 StPO) und stellen Sie das Verfahren mangels hinreichenden Tatverdachts ein, ist ein Wiederaufgreifen der Ermittlungen wegen desselben Tatvorwurfs zwar rechtlich möglich (KK-StPO/*Moldenhauer*, 9. Aufl. 2023, § 170 Rn. 23 m.w.N.). Ergeben sich nach der Verfahrenseinstellung allerdings keine neuen Tatsachen, die einen Anfangsverdacht i.S.d. § 152 Abs. 2 StPO begründen, hat die Einstellungsentscheidung in der Praxis in aller Regel Bestand.

Auch dürfte es die Ausnahme darstellen, dass in derartigen Fällen die gespeicherten Daten für Zwecke der Gefahrenabwehr notwendig sind.

Die Pflicht zur Datenlöschung stellt in solchen Konstellationen mithin den Regelfall, die Befugnis zur Weiterspeicherung den Ausnahmefall dar.<sup>3</sup>

Wird eine einzelfallbezogene Prüfung der Erforderlichkeit der weiteren Datenaufbewahrung als zu aufwendig angesehen, spricht viel dafür, eine *automatische* Löschung nach Ablauf einer bestimmten Frist zu normieren, um einer – in der Regel anzunehmende – unrechtmäßigen Weiterspeicherung vorzubeugen.

Durch einen solchen Mechanismus würden auch die durch die gesetzliche Regelung des § 22 Abs. 2 S. 5 PolG möglichen „Mitzieh-Effekte“ im Rahmen der Bestimmung der Prüfungstermine zur Datenlöschung gemindert. Die Vorschrift besagt, dass, wenn innerhalb der regulären Prüffrist (bei Erwachsenen: 10 Jahre) weitere personenbezogene Daten über dieselbe Person gespeichert werden, für alle Speicherungen gemeinsam der Prüftermin gilt, der als letzter eintritt. Auf diese Weise können, je nach Fallgestaltung, Jahrzehnte vergehen, ohne dass eine turnusmäßige Überprüfung Rechtmäßigkeit der weiteren Datenspeicherung stattfindet, was häufig dazu führen dürfte, dass eigentlich gebotene Datenlösungen unterbleiben.

## II. Zur Informationspflicht

Polizeibehörden sind in Nordrhein-Westfalen derzeit nicht gesetzlich verpflichtet, (ehemals) beschuldigte Personen darüber zu informieren, welche polizeiliche Stelle in welchem Umfang personenbezogene Daten über sie gespeichert hat. Das PolG sieht lediglich unter gewissen Voraussetzungen anlassbezogene Benachrichtigungspflichten im Zusammenhang mit verdeckten und/ oder besonders eingriffsintensiven Maßnahmen (§ 33 PolG) sowie im Fall erheblicher Datenschutzverletzungen (§ 33a PolG) vor.

Auch wenn darüber hinausgehende Informationspflichten nach dem Wortlaut des Art. 13 der JI-Richtlinie nicht zwingend zu normieren sind („...in besonderen Fällen...“), wäre es dem auch der JI- Richtlinie zugrunde liegenden Prinzip der Transparenz der polizeilichen Datenverarbeitung (vgl. Erwägungsgrund 26 der JI-Richtlinie)

---

<sup>3</sup> Wird eine gem. § 170 Abs. 2 StPO erfolgte Verfahrenseinstellung mit der Beschwerde (§ 171 Abs. 1 StPO) angegriffen, ist eine weitere Datenspeicherung für die Dauer des Beschwerde- und eines sich ggf. anschließenden Klageerzwingungsverfahrens freilich notwendig und damit zulässig.

zumindest förderlich, beschuldigten Personen allgemein, d.h. nicht nur in Abhängigkeit von bestimmten Ermittlungsmaßnahmen, die in Art. 13 Abs. 2 der JI-Richtlinie vorgesehenen Informationen, insbesondere die Dauer der Datenspeicherung oder hilfsweise die Kriterien für die Festlegung dieser Dauer, zur Verfügung zu stellen.

Ein derartiges eher weites Verständnis der Informationspflichten nach Art. 13 der JI-Richtlinie liegt auch der Rechtsprechung des EuGH zugrunde, wenn er in dem bereits zitierten Urteil feststellt:

*„Um es den betroffenen Personen insbesondere zu ermöglichen, diese „Angemessenheit“ [der Löschfristen, Anm. d. Verf.] zu überprüfen und gegebenenfalls eine solche Löschung zu beantragen, sehen Art. 13 Abs. 2 Buchst. b und Art. 14 Buchst. d der Richtlinie 2016/680 vor, dass diese Personen grundsätzlich, falls dies möglich ist, über die Dauer, für die die sie betreffenden personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, über die Kriterien für die Festlegung dieser Dauer informiert werden können.“ (EuGH, Urt. v. 30.1.2024 - C-118/22, Rn. 46).*

### **III. Zu einer Zentralstelle für Betroffenenrechte**

Eine effektive Durchsetzung von datenschutzrechtlichen Auskunftsansprüchen gegenüber der Polizei wird in der Praxis häufig durch den Umstand vereitelt, dass die Polizeibehörden über eine Vielzahl unterschiedlicher und unabhängig voneinander geführter Datenbanken und Dateisysteme verfügen, die darüber hinaus z.T. zusammen mit Daten anderer Landes- und Bundespolizeien in Verbunddateien gespeichert werden. Eine einheitliche Überprüfung, Beauskunftung und/ oder Datenlöschung ist deshalb nur schwer ermöglicht. Häufig findet ein erfasster Vorgang Eingang in mehrere unterschiedliche Datenbanken. Zur Bearbeitung von Auskunfts- und Löschanträgen muss dann – nach meiner, auf der Außenperspektive beruhenden Kenntnis – oftmals eine große Zahl von Datenbanken einzeln abgefragt werden und im Fall von Lösungsersuchen einzeln bereinigt werden. Dies betrifft auch Daten, die im Rahmen von Strafverfahren erlangt wurden, da die verwendeten Datenbanken und Verbundsysteme eine strikte Trennung zwischen Daten, die für Zwecke der Strafverfolgung verarbeitet werden, und Daten, die für präventiv-polizeiliche Zwecke verarbeitet

werden, in der Regel nicht vorsehen (sog. „Mischdateien“).<sup>4</sup> Zudem dürfen in Strafverfahren erhobene Daten grds. auch für Zwecke der Gefahrenabwehr verwendet werden und finden dadurch Eingang in präventiv-polizeiliche Datenbanken.

Erschwert wird die erfolgreiche Geltendmachung von Betroffenenrechten zusätzlich durch die Vielzahl von Polizeibehörden innerhalb der Bundesländer, die jeweils für die durch sie vorgenommene Datenverarbeitung verantwortlich sind, und dem Umstand, dass einzelne Behörden jeweils über eigene Datenbestände verfügen, die einem direkten Zugang durch andere Polizeibehörden entzogen sind (z.B. auf lokalen Rechnern und/ oder in behördeneigenen Datenbanken gespeicherte Daten).

Diese Situation hat zur Folge, dass Betroffene in aller Regel nicht wissen, welche Polizeibehörde Daten über sie gespeichert hat. So ist häufig bereits der richtige Adressat eines Auskunfts- und/ oder Löschungsersuchens unklar.

Vor diesem Hintergrund wäre eine zentralisierte Bearbeitung und Durchsetzung von Auskunfts- und Löschanträgen wünschenswert, um die beschriebenen praktischen Hindernisse zu verringern. Anders als derzeit das Landesamt für Zentrale Polizeiliche Dienste sollte eine solche Zentralstelle dabei nicht lediglich als „Verteiler“ von Betroffenenanträgen an die datenschutzrechtlich verantwortlichen Polizeibehörden fungieren, sondern insoweit mit einer eigenständigen Prüf- und Anordnungscompetenz ausgestattet werden, um eine wirksame Rechtsdurchsetzung zu ermöglichen.

Insbesondere bei Daten aus Strafverfahren ist allerdings zu bedenken, dass diese oftmals länderübergreifend verarbeitet werden. Bedient sich etwa eine nordrhein-westfälische Staatsanwaltschaft im Wege der Amtshilfe polizeilichen Ermittlungspersonen in anderen Bundesländern, wie es in der Praxis häufig vorkommt, werden in aller Regel auch dort personenbezogene Daten gespeichert, die der Prüf- und Anordnungscompetenz einer Zentralstelle im Land NRW dann entzogen wären.

Die beschriebenen praktischen Probleme bei der Geltendmachung von Betroffenenrechten würden durch eine zentralisierte Bearbeitung auch aus anderen Gründen nicht vollständig behoben. Entscheidend für eine effektive Auskunftserteilung und Löschung dürfte vielmehr sein, dass durch geeignete Maßnahmen dafür Sorge getragen wird, dass auf operativer Ebene das Gebot der Datensparsamkeit beachtet wird, dass

---

<sup>4</sup> Vgl. dazu Arzt, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Auflage 2021, Kap. G Rn. 1111 ff.

Daten richtig zugeordnet und dass Verarbeitungsvorgänge ordnungsgemäß protokolliert werden. Denn Auskunfts- und Löschungsersuchen können nur dann richtig, vollständig und in angemessener Zeit bearbeitet werden, wenn die verantwortliche Stelle die betreffenden Daten in einem möglichst standardisierten Verfahren zuverlässig identifizieren kann.



Dr. David Albrecht  
Rechtsanwalt